AD-A066 331 MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTE--ETC F/G 12/1
MENTAL POKER,(U)
JAN 79 A SHAMIR, R L RIVEST, L M ADLEMAN N00014-76-C-0366
UNCLASSIFIED MIT/LCS/TM-125 NL

| OF |
AD
A066331

END
DATE
FILMED
5-79
DDC

LABORATORY FOR COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT/LCS/TM-125

MENTAL POKER

Adi Shamir

Ronald L. Rivest

Leonard M. Adleman

29 Jan. ~~February~~ 1979

This report was prepared with the support of National Science Foundation grants No.'s MCS78-05849 and MCS78-04343; and by the Office of Naval Research under contract No. N00014-76-C-0366

545 TECHNOLOGY SQUARE, CAMBRIDGE, MASSACHUSETTS 02139

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
14 1. ~~REPORT NUMBER~~ MIT/LCS/TM-125	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) 6 Mental Poker		5. TYPE OF REPORT & PERIOD COVERED 6. PERFORMING ORG. REPORT NUMBER MIT/LCS/TM-125 ✓
7. AUTHOR(s) 10 Adi Shamir, Ronald L. Rivest [redacted] Leonard M. Adleman		8. ~~CONTRACT OR GRANT NUMBER(s)~~ ✓ ~~NSF~~ MCS78-05849 ~~MCS78-04343~~ 15 N00014-76-C-0366 ✓
9. ~~PERFORMING ORGANIZATION NAME~~ AND ADDRESS MIT/Laboratory for Computer Science ✓ 545 Technology Square Cambridge, MA 02139		10. ~~PROGRAM ELEMENT, PROJECT~~, TASK AREA & WORK UNIT NUMBERS 11
11. CONTROLLING OFFICE NAME AND ADDRESS Associate Program Director/Office of Naval Res. Office Computing Activites/Dept. of the Navy National Sci.Foundation/Information Sys.Program Washington, D. C. 20550/Arlington, VA 22217		12. ~~REPORT DATE~~ 29 Jan[redacted] 1979 13. ~~NUMBER OF PAGES~~ 10
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) 12 11p.		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Poker
cryptography

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Is it possible to play a fair game of "Mental Poker"? We will give a complete (but paradoxical) answer to this question. We will first prove that the problem is intrinsically insoluble, and then describe a fair method of playing "Mental Poker".

409 648

1B

MIT/LCS/TM-125

MENTAL POKER

by
Adi Shamir
Ronald L. Rivest
Leonard M. Adleman

January 29, 1979

This report was prepared with the support of National Science Foundation grants No.'s MCS78-05849 and MCS78-04343; and by the Office of Naval Research under contract No. N00014-76-C-0366.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LABORATORY FOR COMPUTER SCIENCE

CAMBRIDGE MASSACHUSETTS 02139

Mental Poker

by Adi Shamir, Ronald L. Rivest, and Leonard M. Adleman
MIT
Cambridge, Massachusetts 02139
November 29, 1978

Abstract

Can two potentially dishonest players play a fair game of poker without using any cards (e.g. over the phone)?

This paper provides the following answers:

(1) No. (Rigorous mathematical proof supplied.)

(1) Yes. (Correct & complete protocol given.)

Keywords: *Poker, cryptography.*

Once there were two "mental chess" experts who had become tired of their pastime.

"Let's play 'Mental Poker,' for variety" suggested one.

"Sure" said the other. "Just let me deal!"

Our anecdote suggests the following question (proposed by Robert W. Floyd):

Is it possible to play a fair game of "Mental Poker"?

We will give a complete (but paradoxical) answer to this question. We will first prove that the problem is intrinsically insoluble, and then describe a fair method of playing "Mental Poker".

I. What does it mean to play "Mental Poker"?

The game of "Mental Poker" is played just like ordinary poker (see "Hoyle"[2]) except that there are no cards: *all* communications between the players must be accomplished using messages. It may perhaps make the ground rules clearer if we imagine two players, Bob and Alice, who want to play poker over the telephone. Since it is impossible to send playing cards over a phone line, the entire game (including the deal) must be realized using only spoken (or digitally transmitted) messages between the two players.

We assume that neither player is above cheating. "Having an ace up one's sleeve" might be easy if the aces don't really exist! A fair method of playing Mental Poker should preclude any sort of cheating.

A fair game must begin with a "fair deal". To accomplish this, the players exchange a sequence of messages according to some agreed-upon procedure. (The procedure may require each player to use dice or other randomizing devices to compute his hand or the messages he transmits.) Each player must then know which cards are in his hand, but must have no information about which cards are in the other player's hand. The dealing method should ensure that the hands are disjoint, and that all possible hands are equally likely for each player.

During the game the players may want to draw new cards from the "remaining deck", or to reveal certain cards in their hand to the opposing player. They must be able to do so without compromising the security of the cards remaining in their hand.

At the end of the game, each player must be able to check that the game was played fairly and that the other player has not cheated. If one player claimed that he was dealt four aces, the other player must now be able to confirm this.

The above set of requirements makes a "fair game" of Mental Poker look rather difficult to achieve. To make things easier, we'll assume that both players own computers. This enables the use of complicated protocols (say, involving encryption). We do not assume that either player will trust the other's computer. (The players could program their computers to cheat!)

We suggest that you might find it an interesting challenge to attempt to find on your own a method for playing Mental Poker, before reading further.

II. Summary of Results

We will present two results on the problem of playing Mental Poker:

(1) A rigourous proof that it is theoretically impossible to "deal the cards" in a way which simultaneously ensures that the two hands are disjoint and that neither player has any knowledge of the other player's hand (other than that the opponent's hand is disjoint from his).

(2) An elegant protocol for "dealing the cards" that permits one to play a fair game of Mental Poker as desired.

The blatant contradiction between our two results is real in that it is not due to any tricks or faults in either result. We will, in fact, leave to the reader the enjoyable task of puzzling out the differences in underlying assumptions that account for our contradictory results.

III. The Impossibility Proof

For the sake of simplicity, we consider the minimal non-trivial case of dealing two different cards (one to each player) from a deck of three cards {X, Y, Z}. The impossibility proof for this case can be easily generalized to any combination of cards and hand sizes.

If a legal protocol for this case exists, then after exchanging finitely many messages Alice and Bob each know their card but not their opponent's card. These messages must coordinate the two players' choices of cards to prevent them from getting the same card.

Suppose that for a particular "deal"

- the messages exchanged are $M_1, \ldots, M_n$,
- the card Alice actually gets is X , and
- the card Bob actually gets is Y .

We define S_A to be the set of cards that Alice could have gotten in any "deals" where exactly the same messages are exchanged. (Since each player may want to make some random choices in order to get a card which is unpredictable to the other player, different deals could arise with the same sequence of messages being exchanged.) Obviously, the card X is in S_A .

If S_A were to contain just the card X , then the deal would violate our requirement that Bob should have no information about Alice's card. Clearly the sequence of messages uniquely determines Alice's card in this case, so in an information-theoretic sense he has (total) *information about her card.* Furthermore, in any physically-realizable (and terminating) protocol for the deal, Alice has only a finite number of random computations possible, so that Bob can actually determine Alice's card by examining all of them which are consistent with the given message sequence.

On the other hand if S_A contains all three cards, then Bob cannot get any card -- regardless of which card he gets, the message sequence is consistent with the possibility that Alice's card is the same. Consequently, S_A must contain exactly two cards.

The set S_B of cards Bob can get without altering his external behavior is similarly defined, and it must also contain exactly two cards. However, the total number of cards in the deck is three, so that S_A and S_B can not be disjoint. (In our example, Z belongs to both sets.) Thus it could happen that both Bob and Alice get the card Z in the case that the message sequence is M_1, ... , M_n. Thus the protocol cannot guarantee that Bob and Alice will choose distinct cards. We conclude that a fair deal is impossible.

IV. A Protocol for the Deal

The following solution meets all the requirements for the problem. First of all, Bob and Alice agree on a pair of encryption and decryption functions *E* and *D* which have the following properties:

(1) $E_K(X)$ is the encrypted version of a message X under key K,
(2) $D_K(E_K(X)) = X$ for all messages X and keys K,
(3) $E_K(E_J(X)) = E_J(E_K(X))$ for all messages X and keys J and K,
(4) Given X and $E_K(X)$ it is computationally impossible for a cryptanalyst to derive K, for all X and K,
(5) Given any messages X and Y, it is computationally impossible to find keys J and K such that $E_J(X) = E_K(Y)$.

Property (3), the commutativity of encryption, is somewhat unusual but not impossible to achieve. Properties (4) and (5), (especially (4)), essentially state that E is "cryptographically strong" or "unbreakable".

As an example of a function with the above properties, consider

$$E_K(M) \equiv M^K \pmod{n}$$

where n is a large number (prime or composite with a given factorization) which is known to both Bob and Alice, and where

$$\gcd(K, \phi(n)\ ) = 1 \ .$$

($\phi(n)$ is Euler's totient function, which can be easily computed from the prime factorization of n.)

The corresponding decoding function is

$$D_K(C) \equiv C^L \pmod{n},$$

where

$$L \cdot K \equiv 1 \pmod{\phi(n)}.$$

Since

$$E_K(E_J(M)) \equiv E_J(E_K(M)) \equiv M^{JK} \pmod{n},$$

E satisfies property (3). For more details on the cryptographic strength and importance of this function see [1,3,4]. We describe this particular encryption fuction here only to demonstrate that the kind of encryption functions we desire apparently exist; we will not make use of any particular properties this function has other than (1) ... (5).

Once Bob and Alice have agreed on the functions E and D (in our example this means agreeing on p), they choose secret encryption keys B and A respectively. These keys remain secret until the end of the game, when they are revealed to verify that no cheating has occurred.

Bob now takes the fifty-two messages:

"TWO OF CLUBS",
"THREE OF CLUBS",

.

.

.

"ACE OF SPADES"

and encrypts each one (whose bit string is considered as a number) using his key B. (That is, he computes E_B("TWO OF CLUBS"), etc.) He then shuffles (randomly rearranges) the encrypted deck and transmits it all to Alice.

Alice selects five cards (messages) at random and sends them back to Bob; these messages Bob decodes to find out what his hand is. Alice has no way of knowing anything about Bob's hand since the encryption key B is known only to Bob.

Now Alice selects five other messages, encrypts them with her key A, and sends them to Bob. Each of these five messages is now doubly encrypted as $E_A(E_B(M))$, or equivalently $E_B(E_A(M))$, for each M. Bob decrypts these messages obtaining $E_A(M)$ for these five messages and sends them back to Alice. Alice can decrypt them using her key A to obtain her hand. Since Bob does not know A, he has no knowledge of Alice's hand.

Michael Rabin suggested a nice physical analogy for the above process. We can view encryption as equivalent to placing a padlock on a box containing the card. Bob initially locks all the cards in individual undistinguishable boxes with padlocks all of which have key B. Alice selects five boxes to return to him for his hand, and then sends him back five more boxes to which she has also added her own padlock with key A to the clasp ring. Bob removes his padlock from all ten boxes and returns to Alice those still locked with her padlock, for her hand. Notice the implicit use of commutativity in the order in which the padlocks are locked and unlocked.

Should either player desire additional cards during the game, the above procedure can be repeated for each card.

At the end of the game both players reveal their secret keys. Now either player can check that the other was "actually dealt" the cards he claimed to have during play. By property (5) neither player can cheat by revealing a key other than the one actually used (one which would give him a better hand).

The above procedure is easily generalized to handle more than two players, as well. (Details left to the reader.) Another obvious generalization is to use commutative encryption functions in secret communications systems to send arbitrary messages (rather than just card names) over a communications channel which is being eavesdropped.

V. Conclusions

We have proved that the card-dealing problem is insoluble, and then we have presented a working solution to the problem. We leave it to you, the reader, the puzzle of reconciling these results. (Hint: Each player would in fact be able to determine the other player's hand from the available information, if it were not for the enormous computational difficulty of doing so by "breaking" the code.)

VI. Acknowledgements

We should like to thank Robert W. Floyd, Michael Rabin, and Albert Meyer for motivation and valuable suggestions.

VII. References

[1] Diffie, Whitfield and Martin E. Hellman, "New Directions in Cryptography," IEEE Trans. Info. Theory IT-22(Nov. 1976), 644-654.

[2] Morehead, A. H., R. L. Frey, and G. Mott-Smith, The New Complete Hoyle, Garden City Books, Garden City, New York, 1947.

[3] Pohlig, Stephen C. and Martin E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance," IEEE Trans. Info. Theory IT-24(Jan. 1978), 106-110.

[4] Rivest, Ronald L., Adi Shamir, and Leonard M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," CACM 21(Feb. 1978), 120-126.

OFFICIAL DISTRIBUTION LIST

Defense Documentation Center
Cameron Station
Alexandria, VA 22314
12 copies

Office of Naval Research
Information Systems Program
Code 437
Arlington, VA 22217
2 copies

Office of Naval Research
Branch Office/Boston
495 Summer Street
Boston, MA 02210
1 copy

Office of Naval Research
Branch Office/Chicago
536 South Clark Street
Chicago, IL 60605
1 copy

Office of Naval Research
Branch Office/Pasadena
1030 East Green Street
Pasadena, CA 91106
1 copy

New York Area Office
715 Broadway - 5th floor
New York, N. Y. 10003
1 copy

Naval Research Laboratory
Technical Information Division
Code 2627
Washington, D. C. 20375
6 copies

Assistant Chief for Technology
Office of Naval Research
Code 200
Arlington, VA 22217
1 copy

Office of Naval Research
Code 455
Arlington, VA 22217
1 copy

Dr. A. L. Slafkosky
Scientific Advisor
Commandant of the Marine Corps
(Code RD-1)
Washington, D. C. 20380
1 copy

Office of Naval Research
Code 458
Arlington, VA 22217
1 copy

Naval Electronics Lab Center
Advanced Software Technology
Division - Code 5200
San Diego, CA 92152
1 copy

Mr. E. H. Gleissner
Naval Ship Research & Development Center
Computation & Math Department
Bethesda, MD 20084
1 copy

Captain Grace M. Hopper
NAICOM/MIS Planning Branch
(OP-916D)
Office of Chief of Naval Operations
Washington, D. C. 20350
1 copy

Captain Richard L. Martin, USN
Commanding Officer
USS Francis Marion (LPA-249)
FPO New York, N. Y. 09501
1 copy